REMARKS

The Examiner has rejected Claims 1-4, 18-22, 36 and 39 under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (U.S. Patent No. 6,298,445) in view of Fujimori (U.S. Patent No. 6,681,213). The Examiner has further rejected Claims 5-9, 23-27, and 37-38 under 35 U.S.C. 103(a) as being unpatentable over Shostack in view of Fujimori and Applicant Admitted Prior Art. The Examiner has still further rejected Claims 10-14 and 28-32 under 35 U.S.C. 103(a) as being unpatentable over Shostack in view of Fujimori and Mizrachi et al. (U.S. Patent Application Publication No. 2003/0033486). The Examiner has rejected Claims 15-17 and 33-35 under 35 U.S.C. 103(a) as being unpatentable over Shostack in view of Fujimori and in further view of Hopmann et al. (U.S. Patent No. 6,578,069).

Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to independent Claims 1, 18 and 36. Specifically, applicant has amended such claims to include the subject matter of dependent Claim 3 et al.

With respect to all of the independent claims, the Examiner has relied on the following excerpt from Fujimori to make a prior art showing of applicant's claimed "determining whether the risk assessment scan involves an intermediate device coupled between the target and the remote source" (see this or similar, but not identical language in each of the independent claims).

> "Each of the authorized nodes has a normal mode and a protected mode for its data input/output operation. On a communication network constituted only by authorized nodes, each of the nodes is allowed to freely input and output (communicate) data in the normal mode. The monitor node, which is also connected to the communication network, detects when an unauthorized node is connected to the network, and then instructs each of the authorized nodes to input and output data in the protected mode. By thus communicating the data in the protected mode, unauthorized copying of the data by the unauthorized node can be effectively avoided." (Col. 2, lines 1-12)

The Examiner has responded to applicant's arguments by arguing that "Fujimori teaches the monitor node, which is connected to the communication network, remotely detects when an unauthorized node is connected to the network to make unauthorized copying." Applicant respectfully disagrees that such disclosure in Fujimori meets applicant's specific claim language. First, Fujimori only detects unauthorized nodes, and not determining whether a risk assessment scan on the target involves an "intermediate device coupled between the target and the remote source" (emphasis added), as claimed. The Examiner has argued that unauthorized nodes are the same as an intermediate device coupled between the target and the remote source. However, applicant respectfully disagrees as there is not even a suggestion in Fujimori of an unauthorized node coupled *between* the target and the remote source, let alone applicant's determining whether a risk assessment scan on the target involves the unauthorized node, as claimed.

Second, Fujimori merely teaches a monitor node that monitors a network for unauthorized nodes. Clearly monitoring a network does not meet applicant's claimed "initiating a risk assessment scan on a target utilizing a network" (emphasis added). "Monitoring" simply does not rise to the level of specificity of (and thus does not meet) applicant's claimed risk assessment, as claimed.

Also with respect to each of the independent claims, the Examiner has responded to applicant's arguments with regards to the claimed "notifying an administrator if it is determined that the risk assessment scan involves the intermediate device" (see this or similar, but not identical language in each of the independent claims). Specifically, the Examiner has stated that "Shostack teaches notifying/alarming an administrator if intrusion is detected" (Shostack Col. 6, lines 53-56). The Examiner has further stated that the combination of such disclosure in Shostack with Fujimori's "detecting an unauthorized node" (Fujimori Col. 2, lines 5-12) meets applicant's specific claim language.

Applicant respectfully disagrees with the Examiner's assertion that such combined references meet applicant's specific claim language. As admitted by the Examiner, Shostack's alarm only relates to the detection of an intrusion. Fujimori, on the other hand, simply provides monitoring for detecting unauthorized nodes. If Shostack and Fujimori were combined, they would teach sending an alarm upon detection of an unauthorized node, which clearly would not meet applicant's claim language, namely "notifying an administrator if it is determined that the risk assessment scan *on the target* involves the intermediate device" (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite the foregoing paramount distinctions and in the spirit of expediting the prosecution of the present application, applicant has amended independent Claims 1, 18 and 36 to include the subject matter of dependent Claim 3 et al. (the subject matter of which was also originally included in independent Claims 37 and 38).

With respect to former dependent Claim 3 et al., the Examiner has responded to applicant's arguments by stating that Fujimori teaches the first procedure performed on the monitor node and the other procedure is performed on authorized nodes. Applicant respectfully disagrees that such an assertion meets applicant's claimed "plurality of

procedures [that] are utilized to determine whether the risk assessment scan involves the intermediate device."

Specifically, Fujimori simply teaches that the monitor node detects unauthorized nodes. Also, Fujimori teaches that authorized nodes are instructed by the monitoring node to communicate data in protected mode. However, simply detecting unauthorized nodes and instructing an authorized node to communicate in a protected mode does not even relate to a procedure that is utilized "to determine whether the risk assessment scan involves an intermediate device" (emphasis added), as claimed by applicant. Thus, Fujimori does not teach "a plurality of procedures," in the specific context claimed by applicant.

For the same reasons as argued above with respect to dependent Claim 3 et al., applicant also respectfully asserts that the prior art does not meet applicant's claimed "executing a plurality of procedures to determine whether the risk assessment scan on the target involves a proxy server coupled between the target and the remote source" in independent Claims 37 and 38.

In addition, the prior art is further deficient with respect to the dependent claims. For example, with respect to dependent Claim 4 et al., the Examiner has responded to applicant's arguments by stating that Shostack teaches providing a map of all ports on the network and pinging all Internet Protocol devices (Col. 7, lines 5-19). However, applicant respectfully asserts that Shostack's mere mention of mapping ports on a network does not relate to the "port list," in the context of applicant's claims. Specifically, only applicant teaches utilizing a port list to determine whether the risk assessment scan involves the intermediate device.

In addition, applicant again argues that the excerpt from Shostack relied on by the Examiner does not meet applicant's claimed "determining a port list associated with the risk assessment scan" (emphasis added), since Shostack clearly discloses providing a map

of ALL ports on the network, as opposed to those specifically associated with the risk assessment scan.

With respect to dependent Claims 10, 12-14 et al., the Examiner has relied on paragraph [0029] in Mizrachi to make a prior art showing of applicant's claimed technique "wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network" (Claim 10 et al.), "wherein at least one of the procedures further includes analyzing responses to the first and second requests" (Claim 12 et al.), "wherein at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis" (Claim 13 et al.), and "wherein at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different" (Claim 14 et al.).

After careful reviewing such excerpt, however, it is clear that Mizrachi only teaches cache memory that holds information for access by a process in performing tasks, but not that there is any sort of first request for content and second request for a cached version of the content, in the manner claimed by applicant. Furthermore, Mizrachi does not teach that any responses for the requests are analyzed, that an indication is made that a risk assessment scan involves an intermediate device based on the analysis, or that such an indication is specifically made when the responses to the two requests are different.

Further, with respect to dependent Claim 13 et al., the Examiner has relied on Col. 2, lines 1-9 of Fujimori to meet applicant's claim language noted above. Applicant asserts that such excerpt only teaches detecting unauthorized nodes, and not any sort of indication that the risk assessment scan involves the intermediate device based on an analysis, where the analysis is associated with responses for requests for content and a cached version of the content, in the manner claimed by applicant.

With respect to dependent Claims 15-17 et al., the Examiner has relied on the following excerpt from Hopmann to make a prior art showing of applicant's claimed technique "wherein at least one of the procedures includes transmitting a request without specifying a host header value" (Claim 15 et al.), "wherein at least one of the procedures further includes identifying an error message in response to the request" (Claim 16 et al.), and "wherein the at least one of the procedures includes indicating that the risk assessment scan involves the intermediate device if the response includes the error message" (Claim 17 et al.).

> "If client issues a normal PUT request without any headers specific to replication, then the request will have the default behavior as defined by the currently published HTTP and WebDAV drafts except that a DAV Replication compliant server must return the resource tag (resourcetag) and the resource UID (repl-uid) of the affected resource." (Col. 16, lines 6-11)

Applicant respectfully asserts that the headers in the above excerpt from Hopmann only relate to headers specific to replication, and not "host header value[s]," as claimed by applicant. Furthermore, there is simply no teaching or even suggestion of any sort of "error message," as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P012/01.132.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100